

## CLAIMS

What is claimed is:

1. A method of transferring data in a peer-to-peer computer network that includes a first peer node and a second peer node, the method comprising:

5 providing the second peer node a location information of an interception node instead of a location information of the first peer node in a data transfer between the first peer node and the second peer node;

establishing a communication channel between the interception node and the second peer node;

10 receiving the data in the interception; and  
processing the data in the interception node.

2. The method of claim 1 wherein the data are received by the interception node from the second peer node.

3. The method of claim 1 further comprising:

15 establishing a communication channel between the interception node and the first peer node; and

wherein the data are received by the interception node from the first peer node.

4. The method of claim 1 wherein the data comprise a file.

5. The method of claim 1 wherein the location information of the first peer node

20 comprises an IP address and a port number.

6. The method of claim 1 wherein processing the data in the interception node comprises scanning the data for computer viruses.

7. The method of claim 1 wherein processing the data in the interception node comprises filtering the content of the data.

5 8. The method of claim 1 further comprising:

transferring the data from the interception node to the second peer node after the data have been processed in the interception node.

9. The method of claim 1 further comprising:

10 transferring the data from the interception node to the first peer node after the data have been processed in the interception node.

10. A method of transferring a file in a peer-to-peer computer network, the method comprising:

15 redirecting the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node, the first peer node and the second peer node being computers in the peer-to-peer computer network;

processing the file in the interception node; and

transferring the file from the interception node to the second peer node.

11. The method of claim 10 wherein the peer-to-peer computer network includes the  
20 Internet.

12. The method of claim 10 wherein processing the file in the interception node comprises scanning the file for viruses.

13. The method of claim 10 wherein processing the file in the interception node comprises filtering a content of the file.

5 14. The method of claim 10 wherein redirecting the file comprises:

informing the second peer node that an address of the first peer node is that of the interception node.

15. The method of claim 10 wherein transferring the file from the interception node to the second peer node comprises:

10 querying a P2P server for location information of peer nodes involved in a transfer of the file;

based on a response from the P2P server, identifying the second peer node as a node involved in the transfer of the file from the first peer node; and

transferring the file from the interception node to the second peer node.

15 16. A system for transferring data in a peer-to-peer network, the system comprising:

a presence modifier configured to detect a publication of a location information of a first peer node, the presence modifier being configured to provide to a second peer node a location information of an interception node instead of the location information of the first peer node in response to a detection of the publication, the first peer node and  
20 the second peer node being computers in the peer-to-peer computer network.

17. The system of claim 16 further comprising:

a data scanner in the interception node, the data scanner being configured to scan data passing through the interception node.

18. The system of claim 16 wherein the interception node comprises a computer that is separate from the P2P server.

5 19. The system of claim 16 wherein the location information of the first peer node comprises an IP address and a port number.

20. The system of claim 17 wherein the data scanner is configured to scan the data for computer viruses.

21. The system of claim 16 further comprising:

10 of was of a transfer manager in the interception node, the transfer manager being configured to obtain session information from the presence modifier.

22. A method of transferring a file in a peer-to-peer computer network, the method comprising:

15 transferring the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node, the first peer node and the second peer node being computers in the peer-to-peer computer network;

scanning the file for viruses in the interception node; and

transferring the file from the interception node to the second peer node.